RESPONSE TO ANTICIPATION REJECTIONS

HOROWITZ REFERENCE

The sole reference is Horowitz, which is found to be somewhat confusing. Sketches 1 - 3, below, will explain Horowitz, as interpreted by Applicant.

Brief Explanation

In brief, Horowitz allows "smart cards" to communicate with ordinary magnetic stripe readers. Such communication cannot ordinarily occur. Horowitz adds a magnetic stripe to a smart card, and writes data from the electronic memory of the smart card onto the mag stripe. He uses an external electronic device to perform this writing. An ordinary magnetic stripe reader can now read that data on the mag stripe. This will be explained in greater detail.

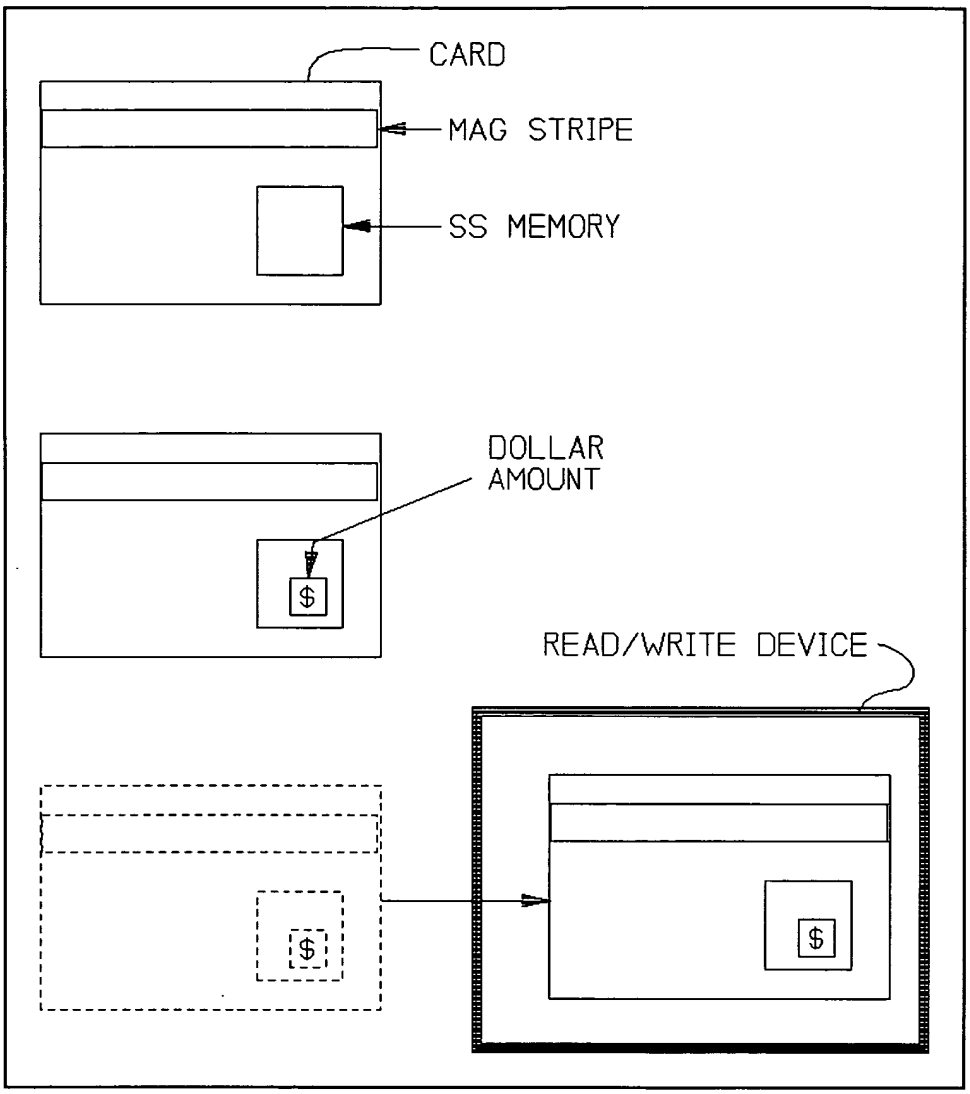
Detailed Explanation

In the top of Sketch 1, below (page 14), a CARD carries an ordinary MAG STRIPE. The CARD corresponds to card 32 in Horowitz's Figure 2. The CARD of Sketch 1 also contains a solid state memory, SS MEMORY. The SS MEMORY corresponds to the Advanced Tech Memory 44 in Horowitz's Figure 2.

In Sketch 1, center, a DOLLAR AMOUNT is loaded into the SS MEMORY. Horowitz states that this loading can be done in numerous

different ways. (Horowitz, page 10, lines 9 - 14; page 10, line 23 - page 11, line 5.) Thus, it is indicated in Sketch 1 as a generic loading operation.

In Sketch 1, bottom, the CARD, now loaded with a dollar amount, is inserted into a READ/WRITE DEVICE. The DEVICE can take the form of PDA 34 in Horowitz's Figure 2, the ATM 38 or the Merchant Terminal 38 of that Figure. (Page 11, lines 6, 7.)



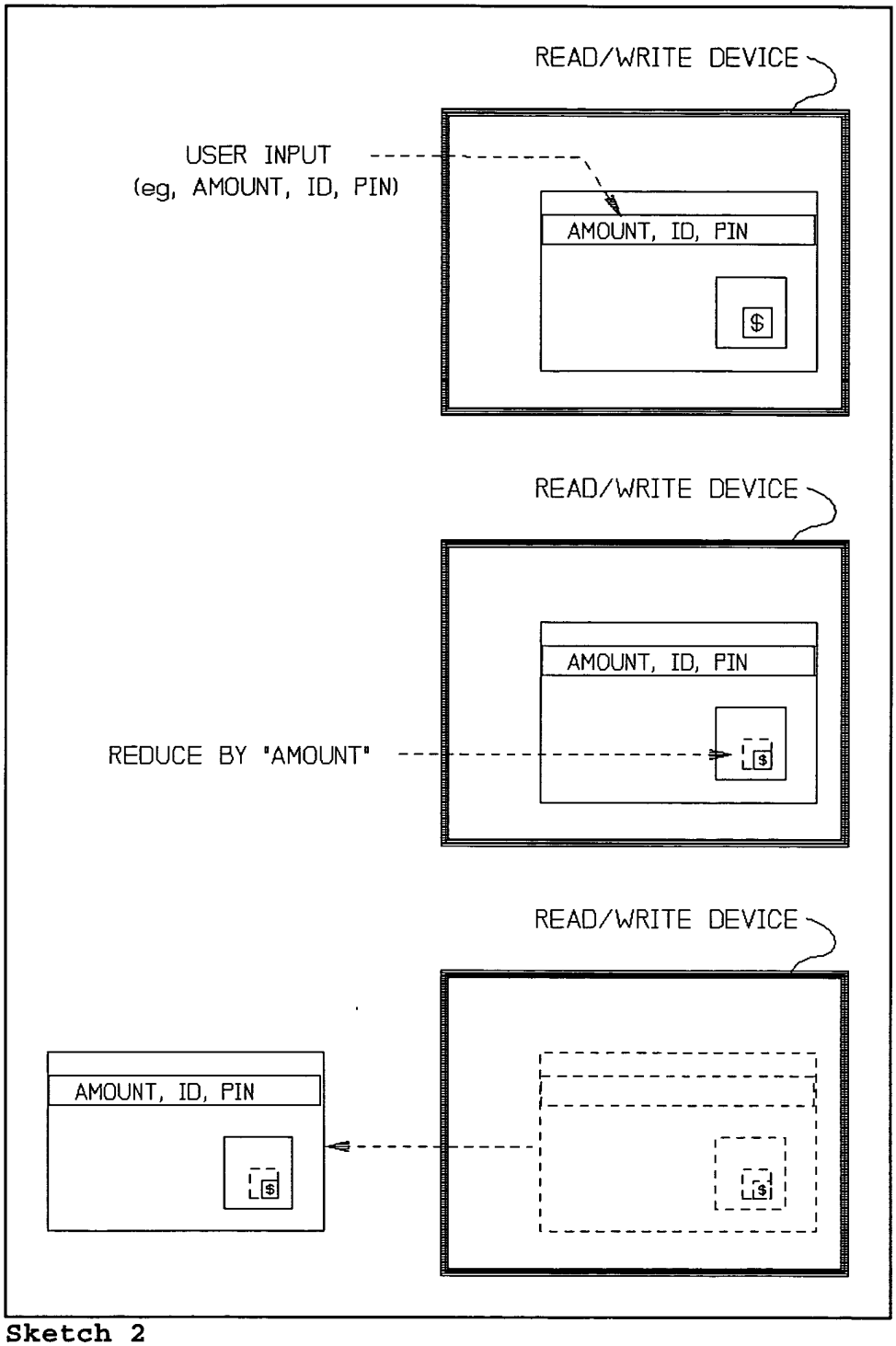
Sketch 1

As indicated in Sketch 2, top, the user then enters various data into the DEVICE, such as an AMOUNT, ID, and PIN. "ID" refers to the identification number of the DEVICE. (Page 11, lines 11 -

14.) "PIN" means Personal Identification Number. The DEVICE writes this data onto the MAG STRIPE. Horowitz calls this data the "special transaction number." (Page 11, line 15.)

As indicated in Sketch 2, center, the DEVICE reduces the DOLLAR AMOUNT previously loaded by the AMOUNT now entered by the user. (Page 11, lines 17 - 19.) In effect, the DOLLAR AMOUNT loaded in Sketch 1, center, represents an amount which is available. The AMOUNT in Sketch 2, top, is an amount to be withdrawn from that dollar amount.

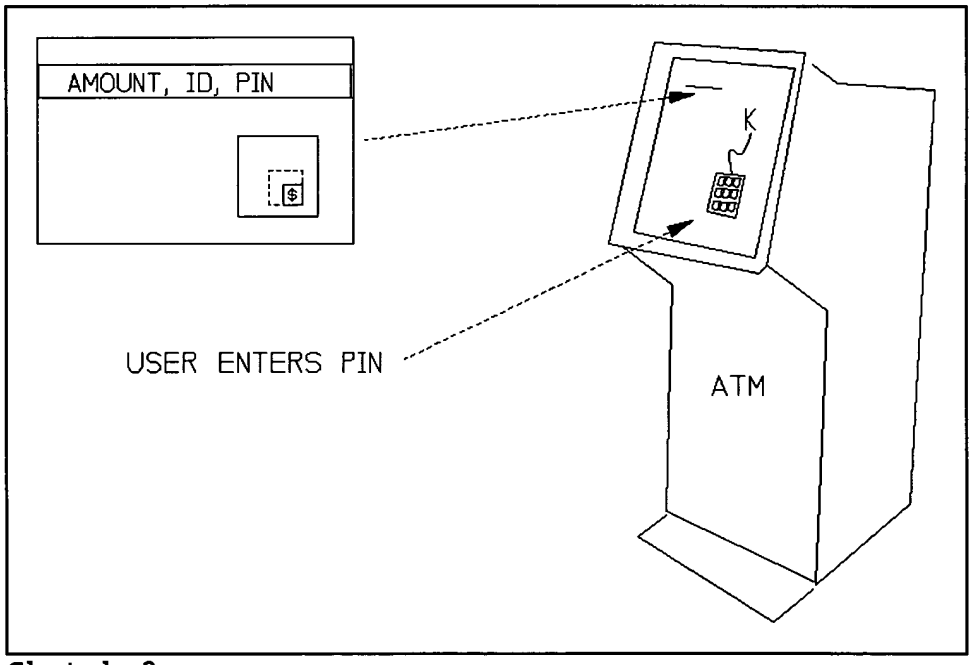
In Sketch 2, bottom, the user withdraws the card from the DEVICE. Now the card has the AMOUNT, ID, and PIN written on the MAG STRIPE


READ/WRITE DEVICE
USER INPUT
(eg, AMOUNT, ID, PIN)
AMOUNT, ID, PIN
$
READ/WRITE DEVICE
AMOUNT, ID, PIN
REDUCE BY "AMOUNT"
$
READ/WRITE DEVICE
AMOUNT, ID, PIN
$
$

Sketch 2

In Sketch 3, the user inserts the card into a kiosk, such as an ATM, Automated Teller Machine. The ATM reads the data on the MAG STRIPE. For example, the AMOUNT may indicate the amount of cash which the ATM is to dispense to the user. (Page 11, line 21 et seq.)

Significantly, the user is required to enter a PIN using the keypad K of the ATM. That PIN must match the PIN written on the MAG STRIPE. (Page 12, line 1 et seq., especially lines 4 - 10.)

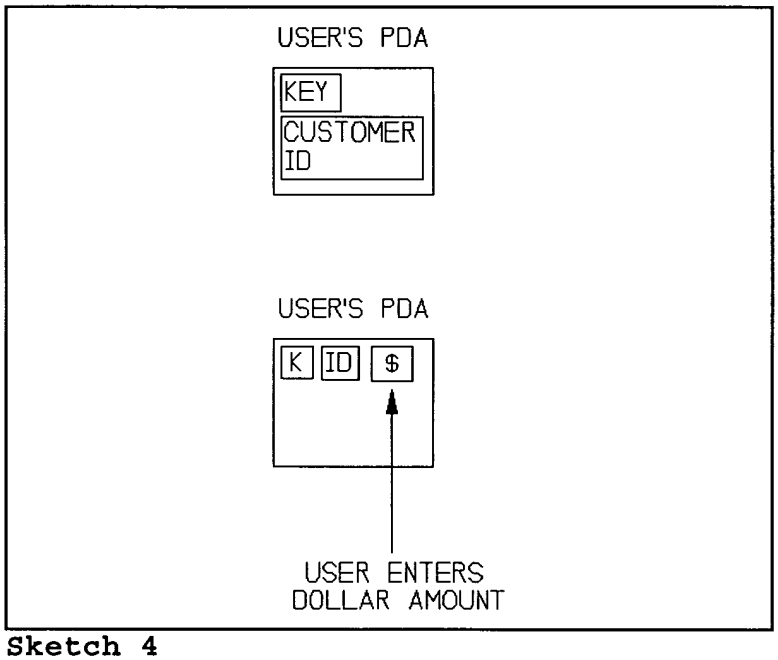


Sketch 3

The Invention, One Embodiment

Sketch 4, top, illustrates the USER'S PDA, Personal Digital Assistant, which can, for present purposes, be viewed as a pocket-sized portable computer. The PDA is equipped with a cryptographic KEY and a CUSTOMER ID.

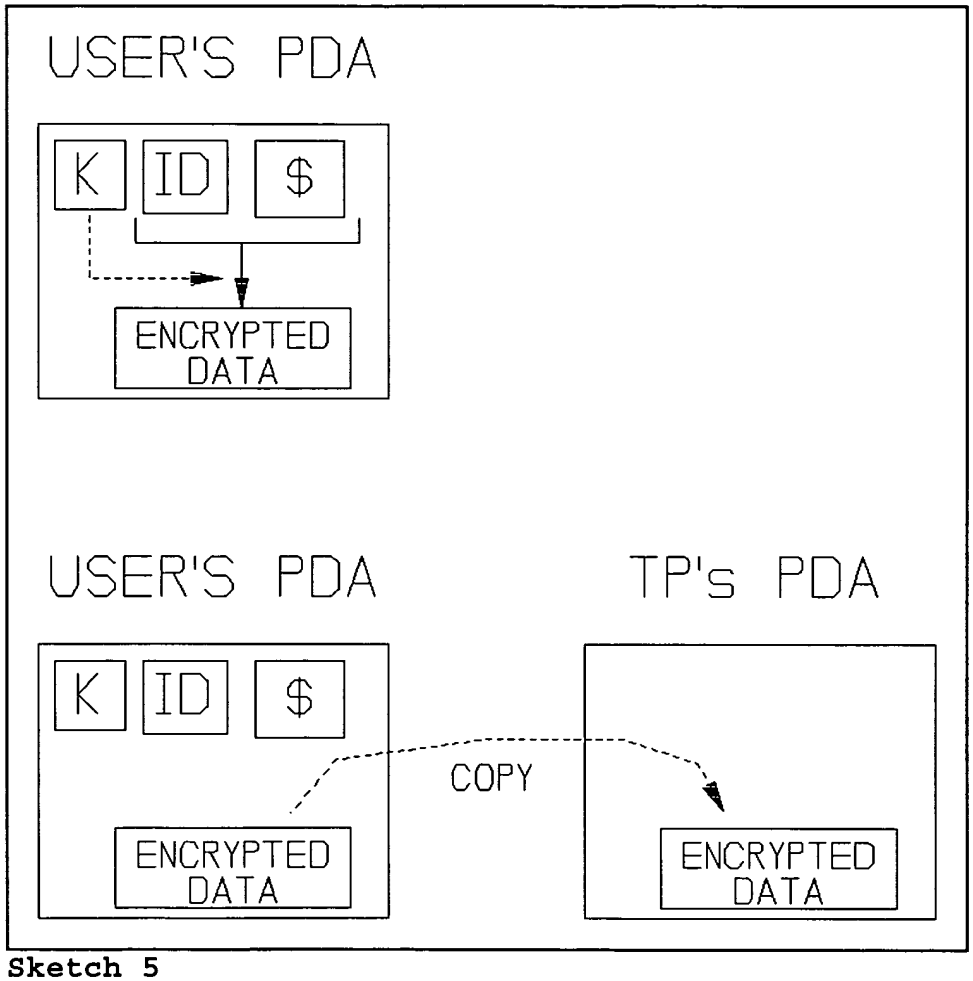
Sketch 4, bottom, shows the KEY as block K and the CUSTOMER ID as block ID. The user enters a DOLLAR AMOUNT, as indicated.



Sketch 4

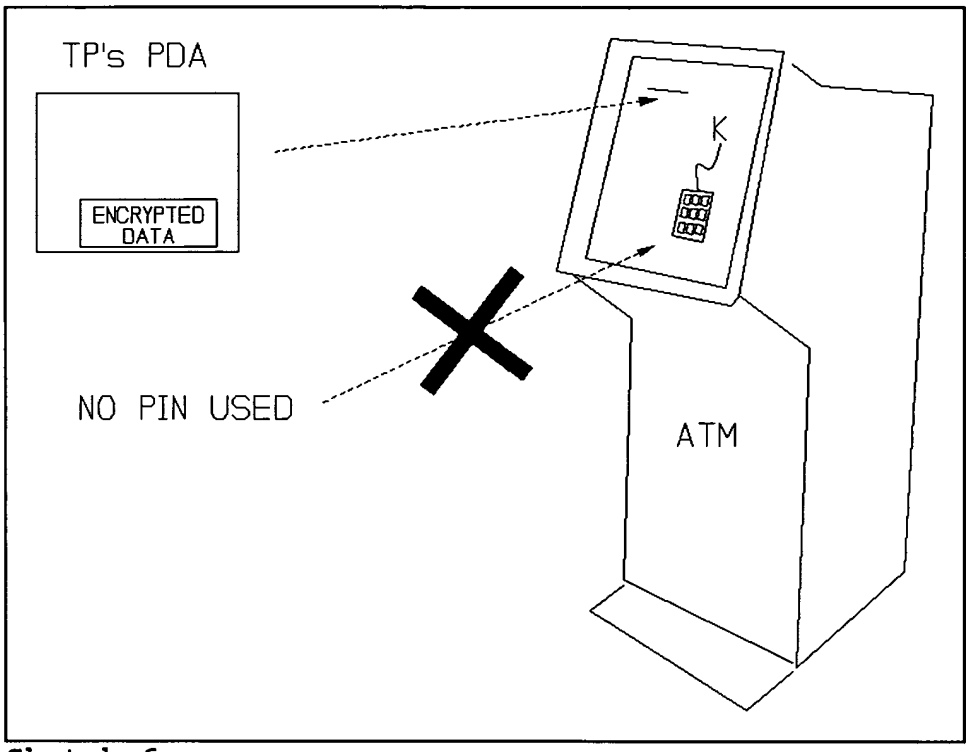
In Sketch 5, top, the USER's PDA encrypts the ID and the dollar amount $, using the key K, to produce ENCRYPTED DATA.

In Sketch 5, bottom, the ENCRYPTED DATA is copied (or transferred without copying) to a third party's PDA, TP's PDA.



Sketch 5

In Sketch 6, the TP's PDA is inserted into a kiosk, such as an ATM. The ATM executes the transaction indicated by the ENCRYPTED DATA, such as dispensing the dollar amount entered in Sketch 4, bottom.



Sketch 6

Two significant features of the invention are that

1) No PIN is required from the third party, so that the third party never gains access to the PIN, so he cannot use it again later, and

2) the ENCRYPTED DATA, by itself, is sufficient to initiate and complete the transaction.

In addition, the operation of invention should be contrasted from another type of operation. A person can give his ATM card and PIN to a third party, to allow the third party to obtain money from an ATM. However, now the third party knows the PIN. Further, the third party can read data from the mag stripe on the ATM card, and create a copy of the ATM card.

In this situation, the third party can raid the account at a later time.

In contrast, under the invention, a user can achieve the same result (allowing the third party to obtain money from the user's ATM account), but the third party obtains no information which could be used later to raid that account. The third party obtains no PIN number, nor access to any information which allows the third party to create a copy of the mag stripe on the ATM card.

RESPONSE TO ANTICIPATION REJECTIONS OF CLAIMS 1 - 13

All claims were rejected on grounds of anticipation, based on Horowitz.

Claim 1

Claim 1 states:

> 1. A method of conducting a transaction via a self service terminal (SST), the method comprising the steps of:
>
> encrypting transaction data stored in a first device under control of a first human party, the data including security identification information;
>
> transferring the encrypted data to a device of a third human party;
>
> transferring or copying the encrypted data from the device of the third human party to the SST; and
>
> causing the SST to decrypt the encrypted data, verify the security identification information, and then execute the transaction upon verification.

An example of the "first device" can be found in Sketch 5 above, top of Sketch, in the form of the user's PDA, which produces the ENCRYPTED DATA.

An example of the "device of a third party" can be found in Sketch 5, bottom, in the TP's PDA.

Applicant points out that no corresponding "first device" and "device of a third party" are found in Horowitz as claimed.

Horowitz may state that the AMOUNT, ID, PIN in Sketch 2, above, can be encrypted onto the MAG STRIPE. (Page 12, bottom.) However, that encrypted data is not "transferred" to "a device of a third party." That encrypted data is written to the card shown in Sketch 2, above, which is returned **to the original user**.

Even if that card is considered a "device," it is not a "third party" "device."

Thus, the claim recitation "transferring the encrypted data to a device of a third party" is missing from Horowitz. MPEP § 2131 states:

> A claim is anticipated only if **each and every element** as set forth in the claim is found, either expressly or inherently described, in a single prior art reference.

Claim 4

Claim 4 recites:

> 4. A method of conducting a transaction via a self service terminal (SST), the method comprising the steps of:
>
> receiving on a third party device encrypted transaction data from a device of a first party, the data including security identification information;
>
> transferring the encrypted data from the third party device to an SST; and
>
> causing the SST to decrypt the encrypted data, verify the security identification information, and then execute the transaction upon verification.

Applicant points out that, in Horowitz, there is no transfer of encrypted data from a first party device to a second party device.

In addition, Applicant points out that the cause-and-effect

relationship of the last paragraph is absent from Horowitz. That paragraph states that, "upon verification" of the "encrypted data" the transaction is executed. Horowitz does not show that.

Horowitz requires that the user enter a PIN. Thus, even if the "encrypted data" in Horowitz is "verified," that is insufficient to execute the transaction. A PIN is still required.

Claim 5

Claim 5 recites:

> ... accepting encrypted transaction data including the identification token from a device of a third party.

Claim 5 also recites a "user," who is given an "encryption key" and an "identification token."

Applicant cannot locate those elements in Horowitz, and requests, under 37 CFR §§ 1.104(c)(2) and 35 U.S.C. § 132, that the PTO specifically identify these elements in Horowitz:

1) the "device of a third party,"

2) the "user,"

3) the "encryption key," and

4) the "token."

Claim 6

Claim 6 recites:

> 6. A method of using a financial service, the method comprising the steps of:
>
> using a device in possession of a first person, encrypting transaction data and an identification token using an encryption key; and
>
> presenting the encrypted data to a financial service operator via a device of a third party.

Applicant cannot locate the "first person," nor the "third party" in Horowitz, and requests that they be identified.

Claim 7

Claim 7 recites:

> 7. A method of purchasing goods or services, the method comprising the steps of:
>
> within a first device, encrypting transaction data permanently stored in the first device, the data including security identification information;
>
> transferring the encrypted data to a device of a third party;
>
> transferring the encrypted data from the device of the third party to a merchant or service provider; and
>
> causing the merchant or service provider to decrypt the encrypted data, verify the security identification information, and then execute the transaction upon verification.

Applicant cannot find the following in Horowitz, and requests

that they be identified:

1) "transaction data" which is "permanently stored" in the "first device,"

2) encrypting the "transaction data" within the "first device,"

3) "transferring the encrypted data to a device of a third party,"

4) the "transferring" of the second-to-last paragraph, and

5) executing the transaction "upon verification."

Claims 8, 10, and 12

Claim 8 recites two persons: a "user" and a "third party." Applicant cannot locate these two claim elements in Horowitz, and requests that they be identified.

This applies to claims 10 and 12.

Claims 10 and 12

Claim 10 recites:

> ... receiving encrypted transaction data including security identification information
>
> from the third party device
>
> which has received the encrypted transaction

> data from a device operated by the ATM customer.

This passage recites two devices: (1) one operated by the third party, and (2) one "operated by the ATM customer."

Applicant cannot locate those two devices in Horowitz, and requests that they be identified.

Similar elements are absent from claim 12, and Applicant asks that those be identified also.

Claim 12

Claim 12 states that

> 1) the retail facility receives encrypted data from a third party device,
>
> 2) the third party device received the encrypted data from a device operated by the customer.

Applicant cannot locate those two devices in Horowitz, and requests that they be identified.

DEPENDENT CLAIMS

The preceding discussion applies to the dependent claims of the claims discussed.

ADDED INDEPENDENT CLAIMS

Claim 17

Claim 17 recites:

> 17. A method, comprising:
>
> a) maintaining a PIN in storage in a user's personal computing device A;
>
> b) entering a dollar amount into the user's personal computing device A;
>
> c) encrypting the dollar amount and the PIN to produce encrypted data;
>
> d) transferring the encrypted data to another computing device B from device A;
>
> e) transferring the encrypted data from the other computing device B to a self-service terminal, SST; and
>
> f) causing the SST, or a related system, to evaluate the PIN in the encrypted data, and if the PIN is valid, executing a transaction involving the dollar amount.

As explained above, in Horowitz, the user enters a dollar amount and a PIN into a card reader, and his smart card writes those items onto a magnetic stripe on the user's card. Applicant fails to see how this shows the overall recitations of claim 17.

Further, Applicant submits that many individual recitations of the claim are not present in Horowitz.

For example, there is no "maintaining a PIN in storage in a user's personal computing device A," as in claim 17(a).

Also, there is no transfer as in claim 17(d).

Claim 19

Claim 19 recites:

> 19. In a process of obtaining currency from an ATM which requires a PIN to dispense currency, a method of delivering a PIN to the ATM, comprising:
>
> a) encrypting a currency amount and a PIN into a packet of encrypted data;
>
> b) delivering the packet to a party who
>
> i) does not know the PIN, and
>
> ii) has no access to the PIN.

Applicant points out that claim 19(b) is directly contrary to Horowitz. Horowitz's party who inserts the card into the ATM must know the PIN, because he is required to enter the PIN into the ATM. (Page 12, top.)

Claim 21

Claim 21 recites:

> 21. A method, comprising:
>
> a) receiving, from a person at an ATM, an encrypted data packet which contains (1) a currency amount and (2) a PIN;
>
> b) without receiving a PIN from the person for confirmation, determining if the encrypted

PIN is valid, and, if so, dispensing currency to the person.

Claim 22(b) is contrary to Horowitz. As explained above, Horowitz requires a PIN from the customer.

CONCLUSION

Applicant requests that the rejections to the claims be reconsidered and withdrawn.

Applicant expresses thanks to the Examiner for the careful consideration given to this case.

Respectfully submitted,

Gregory A. Welte
Reg. No. 30,434

NCR Corporation
1700 South Patterson Blvd.
WHQ - 5E
Dayton, OH 45479
February 17, 2005
(937) 445 - 4956

WELTE DIRECT: (765) 296 - 4699